**Nghiên cứu tấn công DDoS của BONET MIRAI trong IoT**

**Researching DDoS attacks of BONET MIRAI in IoT**

***SV: Lê Quang Long – Nguyễn Thị Lâm Anh – Nguyễn Văn Nam – Võ Tá Trường Tân***

*Lớp 20NS, Khoa Kỹ Thuật Máy Tính Và Điện Tử; Email: lqlong.20it1@vku.udn.vn*

***GVHD: ThS.Ninh Khánh Chi***

*Khoa Kỹ Thuật Máy Tính Và Điện Tử; Email:* [*nkchi@vku.udn.vn*](mailto:nkchi@vku.udn.vn)

***Tóm tắt:*** *Hiện nay Internet of Things (IoT) đang là một xu thế phát triển mạnh trên toàn cầu. Các thiết bị IoT xuất hiện phổ biến và ứng dụng vào hầu hết các lĩnh vực của đời sống, mang lại nhiều lợi ích cho xã hội. Đi kèm với đó là các nguy cơ bị khai thác, đánh cắp dữ liệu hay bị sử dụng cho mục đích trái phép do nhận thức chưa đầy đủ và vấn đề bảo mật còn yếu. Năm 2016, thế giới ghi nhận kỹ thuật tấn công từ chối dịch vụ mới sử dụng mã độc Mirai để điều khiển một mạng BotNet gồm các thiết bị IoT tấn công vào các công ty lớn của Mỹ và Pháp, với băng thông kỷ lục đến 1,5Tbps. Việt Nam là nước có tỉ lệ là nơi xuất phát của các cuộc tấn công sử dụng mã độc Mirai cao nhất trên thế giới. Thông qua đó chúng tôi quyết định sẽ tiến hành “Nghiên cứu tấn công DDoS trong các thiết bị IoT”*

***Từ khóa:*** *DDoS IoT, Botnet Mirai, malware mirai*

***Abstract:*** *Currently, the Internet of Things (IoT) is a growing trend globally. IoT devices appear popular and applied in most areas of life, bringing many benefits to society. Accompanying that is the risk of data being exploited, stolen, or used for unauthorized purposes due to insufficient awareness and weak security issues. In 2016, the world recorded a new denial-of-service attack technique using Mirai malware to control a BotNet network of IoT devices to attack large US and French companies, with a record bandwidth of up to 1.5Tbps. Vietnam is the country with the highest rate of origin of Mirai attacks in the world. Through that, we decided to conduct “DDoS Attack Research in IoT Devices”*

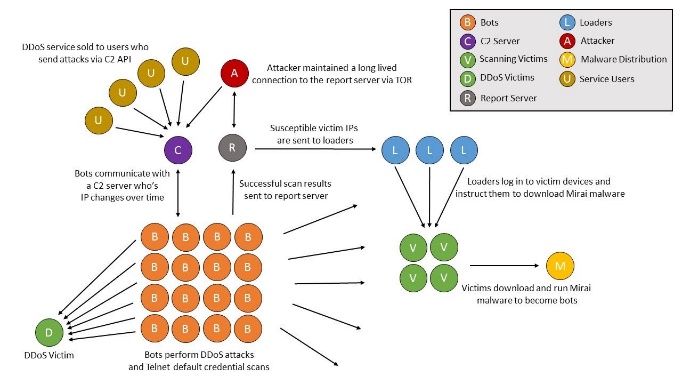
***Key words:***  *DDoS IoT, Botnet Mirai, malware mirai*

# Tổng quan về đề tài nghiên cứu

Ngày nay Internet of Things (IoT) đang là một xu thế phát triển mạnh trên toàn cầu. Các thiết bị IoT xuất hiện phổ biến và ứng dụng vào hầu hết các lĩnh vực của đời sống tiêu biểu như là về nông nghiệp, công nghiệp đặc biệt trong tình hình covid thì IoT được ứng dụng mạnh mẽ trong giáo dục, mang lại nhiều lợi ích cho xã hội. Đi kèm với đó là các nguy cơ bị khai thác, đánh cắp dữ liệu hay bị sử dụng cho mục đích trái phép do nhận thức chưa đầy đủ và vấn đề bảo mật còn yếu. Năm 2016, thế giới ghi nhận kỹ thuật tấn công từ chối dịch vụ mới sử dụng mã độc Mirai để điều khiển một mạng BotNet gồm các thiết bị IoT tấn công vào các công ty lớn của Mỹ và Pháp, với băng thông kỷ lục đến 1,5Tbps. Việt Nam là nước có tỉ lệ là nơi xuất phát của các cuộc tấn công sử dụng mã độc Mirai cao nhất trên thế giới,cũng vào năm 2016 BKAV công bố đến 76% các camera IP đặt mật khẩu là mặt định. Tấn công từ chối dịch vụ (DDoS) và các mạng máy tính ma (Botnet) đang có xu hướng tăng nhanh trên thế giới cũng như tại Việt Nam trong vài năm trở lại đây. Điều này đang đặt ra cho các cơ quan chức năng yêu cầu cấp bách về việc đề ra các giải pháp phối hợp phòng chống botnet và DDoS tại Việt Nam. Phương pháp tấn công mạng APT tuy đã xuất hiện từ lâu, nhƣng gần đây mới được nhiều chuyên gia ATTT nhắc đến, hình thức tấn công này không chỉ nhằm mục đích phá hoại mà còn lấy trộm thông tin. Chúng sử dụng kết hợp nhiều kỹ thuật để tránh sự phát hiện của hệ thống bảo vệ mạng nhằm duy trì sự tồn tại càng lâu càng tốt. Hiện nay, ở Việt Nam chỉ có thể phát hiện và cảnh báo botnet dựa trên các báo cáo nhận được trong giai đoạn 4, 5 (trong chu kỳ một mạng botnet) từ các tổ chức và nạn nhân bị tấn công. Giải pháp này tuy có ưu điểm là chưa cần đầu tư lớn, chi phí vận hành thấp, nhƣng không chủ động phát hiện được sớm và chỉ thu đƣợc thông tin khi mạng botnet bắt đầu thực hiện tấn công mới. Để làm tốt công việc bóc gỡ botnet thì các cơ quan, đơn vị cần có sự phối hợp kịp thời, phải chủ động xây dựng các giải pháp và có kế hoạch phòng chống cụ thể.

# Nội dung và kết quả nghiên cứu

## Các thành phần của mạng lưới Botnet Mirai



* *U: khách hàng thuê mạng Botnet để DDoS*
* *B: các thiết bị IoT bị nhiễm mã độc*
* *C: máy chủ trung gian kết nối attacker và bot*
* *A: attacker người điều khiển mạng Botnet*
* *R: report server nhận thông tin các bot Brute Force thành công*
* *V: các thiết bị IoT mật khẩu mặt định hoặc yếu*
* *D: mục tiêu DDoS*
* *M: mã độc của Botnet Mirai*
* *L: công cụ dùng để lây nhiễm (M) vào (V)*

## Cấu trúc của thư mục Botnet Mirai

Mã nguồn Botnet Mirai được cung cấp trên trang github [*https://github.com/jgamblin/Mirai-Source-Code*](https://github.com/jgamblin/Mirai-Source-Code). Trong đó bao gồm có 2 phần chính là CNC và BOT.

### Chức năng CNC

* Được viết bằng ngôn ngữ Go
* Tạo kết nối trung gian giữa attacker và các bot
* Quan sát và điều khiển mạng lưới Botnet thông qua các lệnh tấn công của atttacker

### Chức năng BOT

* Được viết bằng ngôn ngữ C
* Lắng nghe và thực hiện tấn công từ CNC
* Brute Force các thiết bị IoT trong cùng khu vực mạng và gửi về Report Server (R)

# Kết luận

**Tài liệu tham khảo**

Tarushi Wasson; Tanupriya Choudhury; Shilpi Sharma; Praveen Kumar, (2017), “Integration of RFID and sensor in agriculture using IOT”,2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)

Milica Lekić; Gordana Gardašević, (2018), “IoT sensor integration to Node-RED platform”,2018 17th International Symposium INFOTEH-JAHORINA